ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ชื่อหนังสือ ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย
เรียบเรียงและเผยแพร่โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย.--กรุงเทพฯ :
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๗
๘๔ หน้า. --

ISBN : 978-974-9765-65-4

เลขมาตรฐานสากลประจำหนังสือ ๙๗๘-๙๗๔-๙๗๖๕-๖๕-๔
พิมพ์ครั้งที่ ๑ กันยายน พ.ศ. ๒๕๕๗
จำนวน ๖๐๐ เล่ม
ลิขสิทธิ์ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
พิมพ์ที่ บริษัท เอส.พี.สปีด พริ้นท์ จำกัด
๗๕ /๑ ซอยพิบูลอุปถัมภ์ ถนนลาดพร้าว
แขวงสามเสนนอก เขตห้วยขวาง กรุงเทพมหานคร
โทรศัพท์ ๐๒-๕๑๓-๗๘๙๙
จัดพิมพ์โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี ชั้น ๖
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๕-๙๙ โทรสาร ๐ ๒๑๔๓ ๘๐๓๖-๓๗
เว็บไซต์กระทรวง : http://www.mict.go.th
เว็บไซต์สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ :
http://www.etcommission.go.th

คำนำ

หนังสือ **“ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย”** จัดทำขึ้นเพื่อเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการทำธุรกรรมทางการเงินผ่าน Smartphone ที่ปลอดภัย และสามารถรับมือกับภัยเทคโนโลยีสารสนเทศที่จะมาคุกคามได้ ส่งผลให้ประชาชนเกิดความเชื่อมั่นและมีการทำธุรกรรมทางการเงินผ่าน Smartphone เพิ่มมากขึ้น

คณะผู้จัดทำหวังว่าหนังสือเล่มนี้จะเป็นประโยชน์สำหรับผู้อ่าน และช่วยให้ทุกท่านสามารถทำธุรกรรมทางการเงินผ่าน Smartphone ได้อย่างปลอดภัยมากยิ่งขึ้น

คณะผู้จัดทำ
สิงหาคม ๒๕๕๗

สารบัญ

สารบัญ

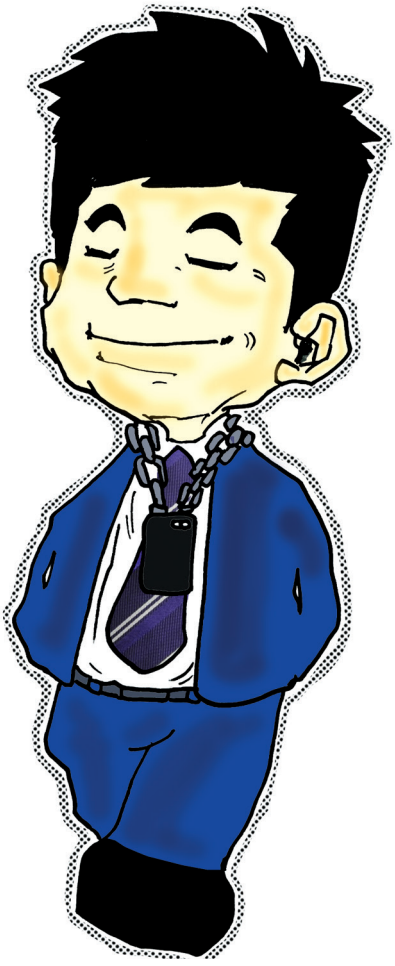
สารบัญ

บทที่ ๑

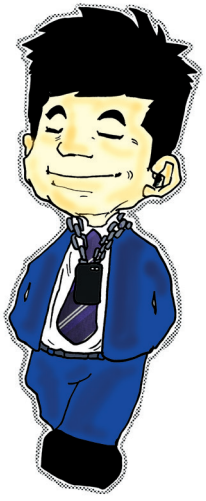
แนวทางการปฏิบัติสำหรับผู้ใช้งาน โทรศัพท์เคลื่อนที่ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย

ธนาคารในยุคใหม่อำนวยความสะดวกสบายให้แก่ผู้ใช้บริการให้สามารถทำธุรกรรมได้ทุกที่ ทุกเวลา แม้กระทั่งในบ้าน แต่ผู้ใช้บริการเองก็ไม่ควรลืมพกพาความปลอดภัยติดตามไปด้วยทุกครั้งที่มีการทำธุรกรรม เพื่อป้องกันภัยร้ายที่อาจแฝงตัวอยู่ในมุมต่างๆ ของโลกออนไลน์ โดยเริ่มจากการศึกษาขั้นตอนการใช้งานอย่างละเอียด เพื่อให้ทราบถึงวิธีการใช้งานที่ปลอดภัย และควรใช้งานด้วยความรอบคอบและระมัดระวังอย่างสม่ำเสมอ ดังนี้

๑. การดูแลรักษาโทรศัพท์เคลื่อนที่อย่างใกล้ชิด



ผู้ใช้งานควรพึงระลึกไว้เสมอว่าความเสียหายที่เกิดขึ้นเมื่อมีการสูญหายหรือโดนขโมยโทรศัพท์เคลื่อนที่ไป จะส่งผลกระทบทั้งในแง่ของทรัพย์สินและข้อมูลที่อยู่ในโทรศัพท์เคลื่อนที่ ยิ่งมีการเก็บข้อมูลสำคัญในโทรศัพท์เคลื่อนที่มากเท่าไรยิ่งมีโอกาสก่อให้เกิดปัญหาตามมามากขึ้นเท่านั้น ยังไม่รวมถึงการเก็บข้อมูลที่เกี่ยวข้องกับองค์กร เช่น อีเมล์ ซึ่งจะส่งผลกระทบกับองค์กรโดยตรง ดังนั้นผู้ใช้งานควรมีความรอบคอบและระวังรักษาโทรศัพท์เคลื่อนที่อย่างใกล้ชิด



๒. การตั้งค่าการล็อกโทรศัพท์เคลื่อนที่เมื่อไม่ใช้งาน

แม้การล็อกการใช้งานโทรศัพท์เคลื่อนที่จะไม่ได้เป็นการป้องกันการเข้าถึงข้อมูลที่ได้ผลร้อยเปอร์เซ็นต์ แต่ก็สามารถเป็นแนวทางเบื้องต้นในการชะลอหรือป้องกันการเข้าถึงข้อมูลสำคัญบนโทรศัพท์เคลื่อนที่จากผู้ไม่หวังดี ซึ่งอาจจะเกิดจากการถูกขโมยโทรศัพท์เคลื่อนที่ และยังเป็นแนวทางที่ผู้ใช้งานสามารถทำได้โดยง่าย ซึ่งกระบวนการดังกล่าวสามารถทำได้โดยการตั้งค่า PIN หรือรหัสผ่านบนโทรศัพท์เคลื่อนที่นั้นๆ (วิธีการสามารถตรวจสอบจากเว็บไซต์ผู้ผลิตโทรศัพท์เคลื่อนที่นั้นๆ หรือสอบถามที่ศูนย์บริการโทรศัพท์เคลื่อนที่ที่ซื้อมา)

๓. การสำรองข้อมูลจากโทรศัพท์เคลื่อนที่ไว้ในแหล่งอื่นที่ปลอดภัย

การสำรองข้อมูลถือเป็นเรื่องที่สำคัญที่ต้องมีการปฏิบัติอยู่เสมอ เนื่องจากเมื่อเกิดเหตุฉุกเฉิน เช่น โทรศัพท์เคลื่อนที่หาย หรือโทรศัพท์เคลื่อนที่ชำรุดหรือใช้งานไม่ได้ ปัญหาอย่างแรกที่จะตามมานอกจากการทำให้โทรศัพท์เคลื่อนที่กลับมาใช้งานได้หรือหาโทรศัพท์เคลื่อนที่ให้พบ คือ การเข้าถึงข้อมูลบนโทรศัพท์เคลื่อนที่ เช่น ข้อมูลผู้ติดต่อ (Contact Book) ซึ่งข้อดีของการสำรองข้อมูล คือ นอกจากจะมีข้อมูลที่สามารถใช้ได้เมื่อเกิดกรณีฉุกเฉินแล้ว ยังทำให้รู้ขอบเขตของข้อมูลที่สูญหายไปด้วย เช่น อาจจะเก็บข้อมูลเลขที่บัญชีธนาคารและรหัสผ่านของธุรกรรมทางอิเล็กทรอนิกส์ (e – Transaction) เอาไว้ ทำให้สามารถแจ้งระงับการเข้าใช้งานได้ก่อนจะเกิดความเสียหาย ซึ่งกระบวนการสำรองข้อมูลของโทรศัพท์เคลื่อนที่แต่ละยี่ห้อหรือแต่ละรุ่นอาจมีความแตกต่างกันไป (วิธีการสามารถตรวจสอบจากเว็บไซต์ผู้ผลิตโทรศัพท์เคลื่อนที่นั้นๆ หรือสอบถามที่ศูนย์บริการโทรศัพท์เคลื่อนที่ที่ซื้อมา)

๔. การพิจารณาเก็บเฉพาะข้อมูลที่จำเป็นในโทรศัพท์เคลื่อนที่

การเก็บข้อมูลบนโทรศัพท์เคลื่อนที่ ควรพิจารณาถึงความสำคัญและความเหมาะสมของข้อมูลที่จะจัดเก็บ ไม่ควรเก็บข้อมูลที่มีความสำคัญมากๆ เช่น ข้อมูลบัตรเครดิต หรือข้อมูลรหัสผ่านสำหรับล็อกอินเข้าใช้งานระบบ เนื่องจากหากโทรศัพท์เคลื่อนที่เกิดสูญหายหรือโดนผู้ประสงค์ร้ายลักลอบขโมยไป อาจทำให้เกิดความเสียหายที่รุนแรงมากกว่าเดิม แต่ในปัจจุบันผู้พัฒนาโปรแกรมบนระบบปฏิบัติการบนโทรศัพท์เคลื่อนที่ต่างๆ ได้พัฒนาโปรแกรมสำหรับจัดเก็บข้อมูลส่วนตัวออกมามากมายและมีการรักษาความมั่นคงปลอดภัยของข้อมูล ทำให้ข้อมูลสำคัญเหล่านี้สามารถเก็บบนโทรศัพท์เคลื่อนที่ได้

๕. การปิดโหมดการเชื่อมต่อบลูทูธหรือหลีกเลี่ยงการเชื่อมต่อบลูทูธจากแหล่งที่มาที่ไม่รู้จัก

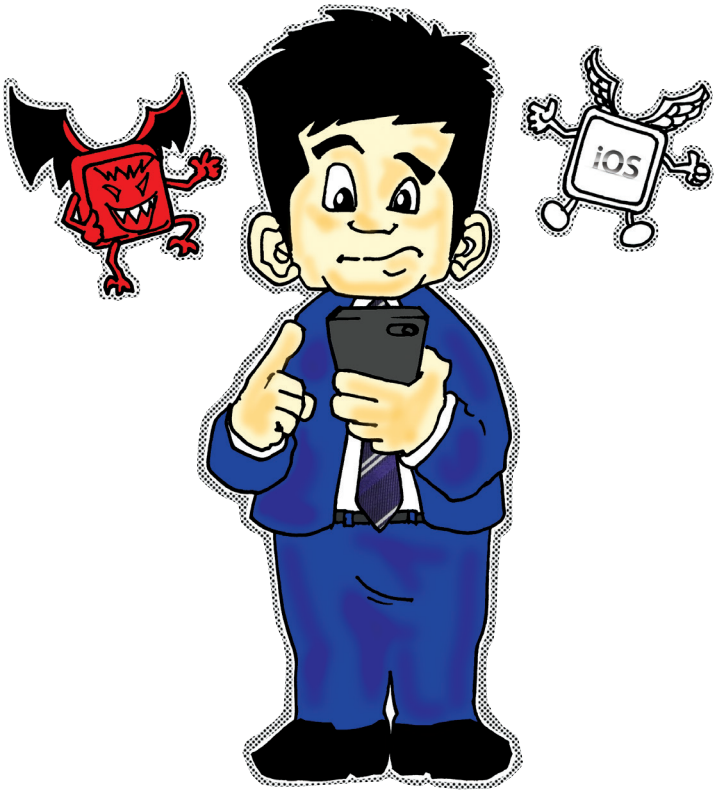
ปัจจุบันผู้ใช้งานมักมีการใช้งานการเชื่อมต่อบลูทูธบนโทรศัพท์เคลื่อนที่ในหลายด้าน เช่น ใช้สำหรับการรับส่งไฟล์ระหว่างโทรศัพท์เคลื่อนที่กับเครื่องคอมพิวเตอร์ หรือใช้สำหรับเป็นโมเด็มเพื่อให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ที่เชื่อมต่อบลูทูธอยู่ ซึ่งหากเป็นการใช้งานตามปกติกับอุปกรณ์หรือบุคคลต่างๆ ที่รู้จักและรับทราบถึงจุดประสงค์ในการเข้าใช้งานการเชื่อมต่อนั้นๆ ก็อาจไม่ก่อให้เกิดผลเสีย แต่ผลเสียจะเกิดต่อเมื่อไม่ทราบว่าผู้ที่ต้องการเชื่อมต่อบลูทูธกับโทรศัพท์เคลื่อนที่ของเรานั้นเป็นใครและมีจุดประสงค์ในการใช้อย่างไร เนื่องจากผู้ไม่หวังดีส่วนใหญ่มักจะอาศัยความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานในการลักลอบใช้งานหรือดึงข้อมูลสำคัญบนโทรศัพท์เคลื่อนที่ เช่น รูปภาพหรือข้อความที่ส่งผ่านทางโทรศัพท์เคลื่อนที่ (SMS : Short Message Service) ไปได้ ซึ่งข้อดีของการใช้งานเครือข่ายบลูทูธคือจะต้องได้รับการยินยอมให้มีการเชื่อมต่อก่อนจึงจะสามารถเชื่อมต่อได้ ซึ่งหากผู้ใช้งานมีความรู้เท่าทันผู้ไม่หวังดี ก็จะทำให้การใช้งานโทรศัพท์เคลื่อนที่มีความ

มั่นคงปลอดภัยมากขึ้น โดยหากไม่มีการใช้งานบลูทูธก็ควรปิดโหมดการเชื่อมต่อบลูทูธไว้ เนื่องจากในบางครั้งอาจพบว่าผู้ใช้งานไม่ได้ตั้งใจกดยอมรับการเชื่อมต่อแต่พลาดไปสัมผัสในขณะที่โทรศัพท์เคลื่อนที่อยู่ในกระเป๋า การปิดโหมดเชื่อมต่อบลูทูธของโทรศัพท์เคลื่อนที่ปกติสามารถเข้าตรวจสอบได้จากเมนู “การเชื่อมต่อ” ซึ่งแต่ละยี่ห้อหรือแต่ละรุ่นอาจมีความแตกต่างกันไป (วิธีการสามารถตรวจสอบจากเว็บไซต์ผู้ผลิตโทรศัพท์เคลื่อนที่นั้นๆ หรือสอบถามที่ศูนย์บริการโทรศัพท์เคลื่อนที่ที่ซื้อมา)

๖. การแจ้งผู้ให้บริการต่างๆ ที่เกี่ยวข้อง เมื่อโทรศัพท์เคลื่อนที่สูญหาย

เมื่อพบว่าโทรศัพท์เคลื่อนที่สูญหายไม่ว่าจะด้วยกรณีโดนขโมยหรือทำตกหล่นที่ใดก็ตาม สิ่งแรกที่ผู้ใช้งานโทรศัพท์เคลื่อนที่ควรทำคือการแจ้งไปยังผู้ให้บริการรายต่างๆ เพื่อปิดบริการและป้องกันความเสียหายที่อาจจะเกิดขึ้น โดยขอบเขตการแจ้งปิดบริการตามรายการข้อมูลที่มีอยู่ในโทรศัพท์เคลื่อนที่นั้นๆ เช่น แจ้งผู้ให้บริการสัญญาณโทรศัพท์เคลื่อนที่ที่ใช้งาน ระงับสัญญาณโทรศัพท์เคลื่อนที่ของตนเองชั่วคราวเพื่อป้องกันการใช้งาน หรือหากมีการเก็บข้อมูลรหัสผ่านของระบบต่างๆ ไว้ในโทรศัพท์เคลื่อนที่ ก็ควรแจ้งปิดการใช้งานด้วย เช่น แจ้งปิดการใช้งานระบบของธุรกรรมทางอิเล็กทรอนิกส์ (e – Transaction) ชั่วคราว แจ้งผู้ดูแลระบบอีเมล์ขององค์กรเพื่อเปลี่ยนรหัสผ่าน เป็นต้น

๗. การเลือกติดตั้งโปรแกรมในโทรศัพท์เคลื่อนที่เท่าที่จำเป็นและจากแหล่งที่มาที่น่าเชื่อถือ



แม้ระบบปฏิบัติการบนโทรศัพท์เคลื่อนที่ทั่วไปจะอนุญาตให้สามารถติดตั้งโปรแกรมเสริมเพื่ออำนวยความสะดวกในการใช้งานมากขึ้น แต่ก็มีความเสี่ยงที่ผู้ใช้งานจะพบกับโปรแกรมที่มีความสามารถในการขโมยข้อมูลหรือโปรแกรมไม่พึงประสงค์ต่างๆ ดังนั้นวิธีการป้องกันที่ดีที่สุดคือดาวน์โหลดเฉพาะโปรแกรมที่จำเป็นจริงๆ และพิจารณาดาวน์โหลดจากเว็บไซต์ของผู้พัฒนาเท่านั้น หรือดาวน์โหลดจากแหล่งดาวน์โหลดที่ได้รับการควบคุมและรับรองความมั่นคงปลอดภัยจากผู้พัฒนาระบบปฏิบัติการ เช่น Android Market สำหรับระบบปฏิบัติการ Android หรือ App Store สำหรับระบบปฏิบัติการ iOS

๘. การควบคุมการเข้าถึงระบบงานต่างๆ ภายในองค์กรเมื่อมีการใช้งานผ่านทางโทรศัพท์เคลื่อนที่

องค์กรควรมีส่วนช่วยในการกำหนดขอบเขตการใช้งานหรือแนะนำแนวทางการปฏิบัติในการเข้าถึงระบบงานต่างๆ ภายในองค์กร เพื่อให้เกิดการรักษาความมั่นคงปลอดภัยในการใช้งานโทรศัพท์เคลื่อนที่อย่างเหมาะสม เช่น พัฒนาระบบการทำงานที่สามารถเข้าถึงได้จากโทรศัพท์เคลื่อนที่ผ่านช่องทางการเข้ารหัสแบบ HTTPS (Hypertext Transfer Protocol Secure) หรือจัดหาช่องทางการใช้งาน VPN (Virtual Private Network) เพื่อเชื่อมต่อเข้าระบบงานภายในองค์กร เป็นต้น

๙. การพิจารณาลิงค์ที่อยู่บนเว็บไซต์ ก่อนการคลิกทุกครั้ง

ภัยคุกคามที่เกิดขึ้นจากการใช้งานเว็บไซต์สามารถเกิดขึ้นได้ง่ายและส่งผลกระทบต่อผู้ใช้งานได้มากที่สุด เนื่องจากโดยส่วนใหญ่เป็นการโจมตีโดยใช้เทคนิคทางจิตวิทยาซึ่งไม่จำเป็นต้องใช้ความรู้ทางเทคนิคมากนัก ผู้ใช้งานโดยส่วนใหญ่ที่ตกเป็นเหยื่อมักจะไม่รู้เท่าทันวิธีการของผู้โจมตี ผู้โจมตีจะใช้เทคนิคต่างๆ หลอกล่อให้ผู้ใช้งานคลิกไปยังลิงค์เพื่อส่งต่อไปยังเว็บไซต์ที่มีอันตราย ดังนั้นทางที่ดีที่สุดคือการใช้วิจารณญาณก่อนคลิกไปที่ลิงค์ใดๆ

๑๐. การอัพเดทระบบปฏิบัติการหรือโปรแกรมบนโทรศัพท์เคลื่อนที่ที่ใช้อยู่ให้เป็นเวอร์ชันใหม่อย่างสม่ำเสมอ

โดยปกติหากมีการดาวน์โหลดโปรแกรมจากผู้พัฒนาต่างๆ และโปรแกรมเหล่านั้น มีการปรับปรุงเกิดขึ้น จะมีการแจ้งอัพเดทโปรแกรมผ่านทางช่องทางต่างๆ เช่น อีเมล์ หรือผ่านระบบแจ้งเตือนของตัวระบบปฏิบัติการเอง เนื่องจากส่วนใหญ่การปรับปรุงเวอร์ชันใหม่ของโปรแกรมต่างๆ จะทำเพื่อปรับปรุงช่องโหว่หรือความผิดพลาดที่เกิดขึ้นในโปรแกรมเวอร์ชันก่อนหน้า ดังนั้นเมื่อผู้พัฒนามีการปรับปรุงเวอร์ชันของโปรแกรม ผู้ใช้ก็ควรทำการอัพเดทโปรแกรมนั้นๆ ให้เป็นเวอร์ชันล่าสุดโดยทันที

๑๑. การใช้โทรศัพท์เคลื่อนที่ทำธุรกรรมออนไลน์อย่างระมัดระวัง

การใช้โทรศัพท์เคลื่อนที่ในการทำธุรกรรมออนไลน์กับหน่วยงานทางการเงินที่ให้บริการผ่านเว็บไซต์สร้างความสะดวกสบายให้กับผู้ใช้งานในการทำธุรกรรมเพิ่มขึ้น แต่การทำธุรกรรมผ่านทางโทรศัพท์เคลื่อนที่ควรเลือกใช้ผู้ให้บริการอินเทอร์เน็ตไร้สายที่มีความน่าเชื่อถือ และเลือกอยู่ในบริเวณที่ผู้ไม่ประสงค์ดีไม่สามารถแอบมองและขโมยข้อมูลส่วนตัวที่สำคัญ (Eavesdropping) เพราะหากผู้ใช้มองข้ามและเลือกใช้เครือข่ายที่ไม่น่าเชื่อถือ อาจถูกโจรกรรมข้อมูลผ่านเครือข่ายได้

บทที่ ๒

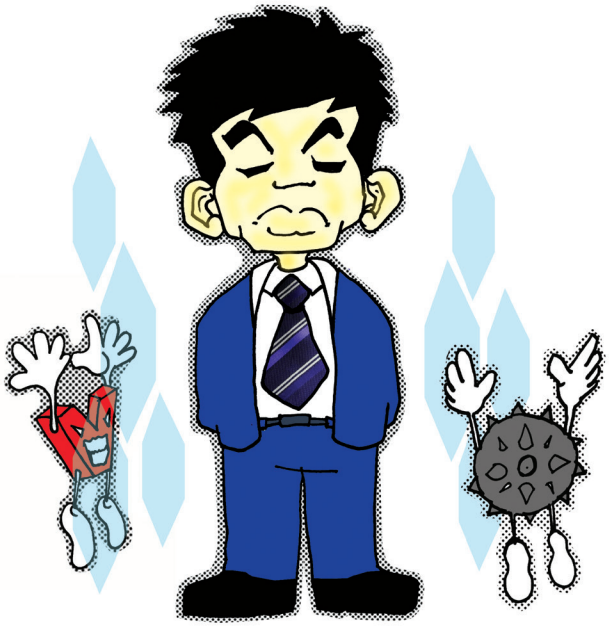
แนวทางการปฏิบัติสำหรับผู้ใช้งานโทรศัพท์เคลื่อนที่ เพื่อให้มีความปลอดภัยในโลกออนไลน์

๑. การป้องกันโทรศัพท์เคลื่อนที่ให้ห่างไกล จากไวรัส โทรจันหรือสปายแวร์

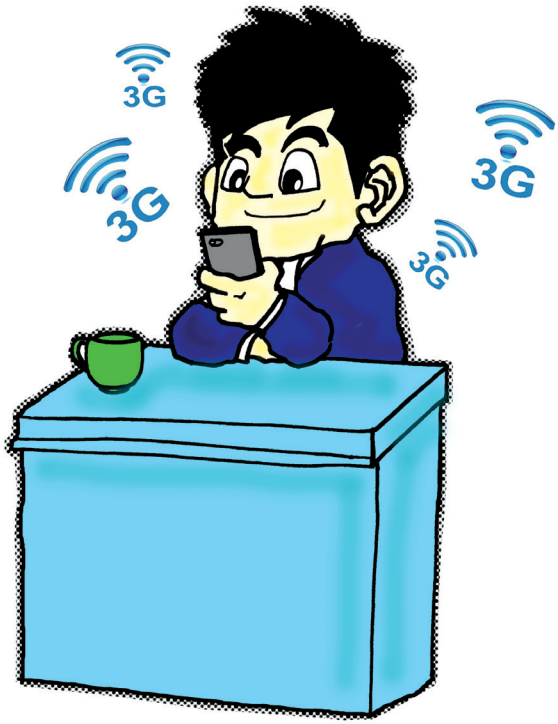
หลีกเลี่ยงการคลิกลิงค์ที่แนบมากับอีเมล์ เพื่อเป็นการป้องกันไม่ให้เผลอคลิกเข้าสู่เว็บไซต์ปลอมที่กลุ่มผู้กระทำการทุจริตนั้นเตรียมไว้

หลีกเลี่ยงการดาวน์โหลดและติดตั้งระบบปฏิบัติการและโปรแกรมที่ไม่มีลิขสิทธิ์ หรือข้อมูลจากเว็บไซต์ที่ไม่น่าเชื่อถือและไม่มั่นใจในความปลอดภัย เพื่อป้องกันโทรจันหรือสปายแวร์ที่อาจแฝงอยู่ในโปรแกรม

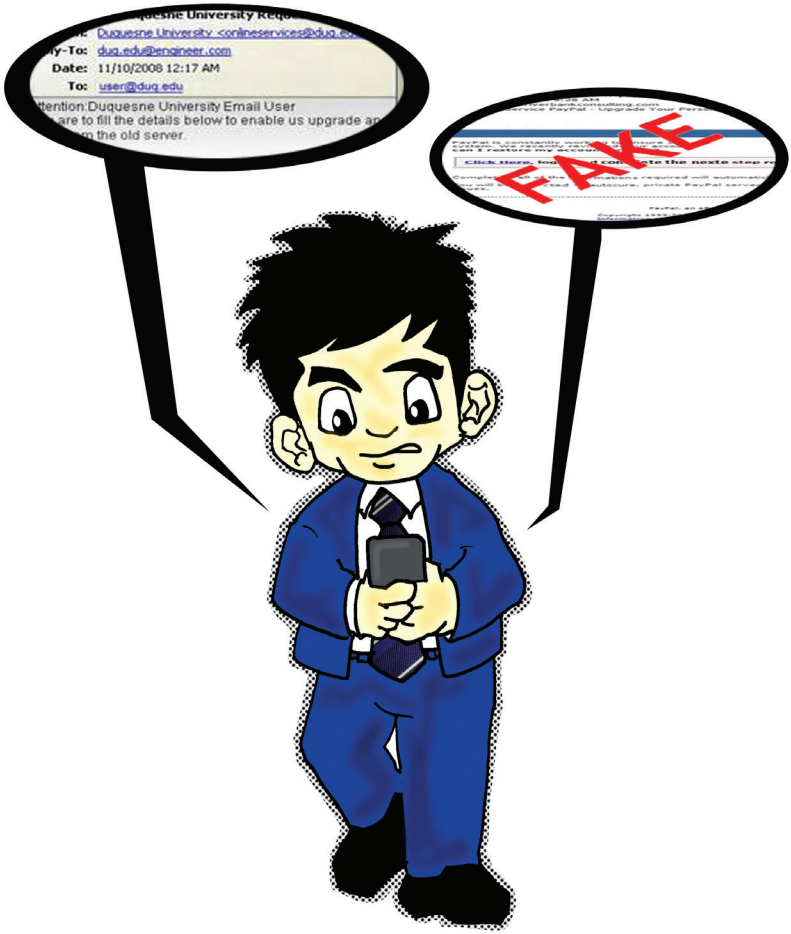
ติดตั้งซอฟต์แวร์ป้องกันไวรัส (Anti - Virus) ที่ถูกลิขสิทธิ์และเชื่อถือได้ และควรตรวจสอบโปรแกรมป้องกันไวรัส และทำการอัพเดทฐานข้อมูลไวรัสให้เป็นเวอร์ชันล่าสุดอยู่เสมอ เพื่อปิดช่องโหว่ที่ไวรัสและมัลแวร์อาจใช้เป็นช่องทางบุกรุกเข้าสู่ระบบ



หากต้องการทำธุรกรรมทางการเงิน ให้ใช้โทรศัพท์เคลื่อนที่ของตนเอง และระมัดระวังการเชื่อมต่อกับเครือข่ายไร้สาย (WiFi) สาธารณะหรือเครือข่ายที่ไม่ปลอดภัย เช่น ในอินเทอร์เน็ตคาเฟ่ เพราะอาจเชื่อมต่อกับเครือข่ายไร้สาย (WiFi) ปลอมที่อาชญากรสร้างขึ้นมา



๒. การสังเกตอีเมล์ปลอม

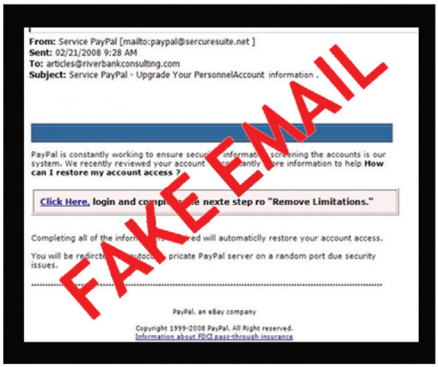


พิจารณาชื่อบัญชีอีเมล์ (e - Mail Address) ว่าเป็นขององค์กรหรือเจ้าหน้าที่ขององค์กรที่ถูกแอบอ้างจริงหรือไม่ หากเป็นองค์กรหรือเจ้าหน้าที่ขององค์กรจริง ชื่อบัญชีอีเมล์มักต่อท้ายด้วยชื่อย่อขององค์กรนั้นๆ เช่น **xxx@mict.go.th** เป็นบัญชีอีเมล์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยย่อมาจาก **Ministry of Information and Communication Technology** เป็นต้น แต่ควรตรวจสอบควบคู่ไปกับลิงค์เชื่อมโยงที่แนบมากับอีเมล์ด้วย

เข้าสู่หน้าเว็บไซต์ด้วยการพิมพ์ที่อยู่ (URL : Uniform Resource Locator) โดยตรงด้วยตัวเองทุกครั้งที่ต้องการใช้บริการธนาคารออนไลน์ และตรวจสอบชื่อเว็บไซต์ในช่องที่อยู่ (Address) ให้แน่ใจก่อนล็อกอิน เพื่อให้มั่นใจว่าได้เข้าสู่เว็บไซต์นั้นอย่างแท้จริง


Enabling...
https://mail.google.com/
misc
BML
study
web me
!!!
Gmail
Calendar
Documents
Photos
Reader
Gmail
by Google
BETA
« Back to

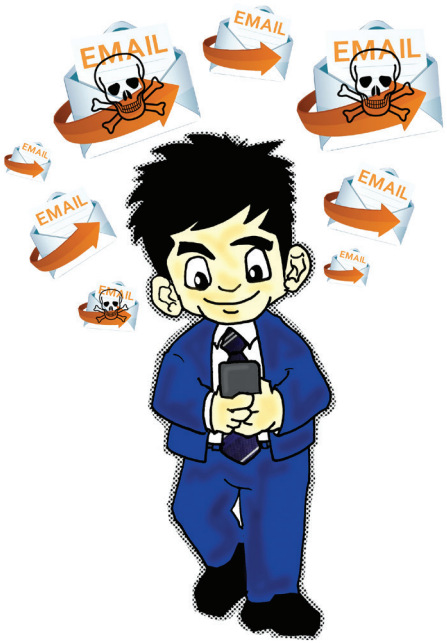
ตรวจสอบลิงค์เชื่อมโยงเว็บไซต์ว่าที่อยู่ (URL : Uniform Resource Locator) ที่ให้เชื่อมโยงไปนั้น เป็นของเว็บไซต์ที่เราเคยใช้บริการอยู่เป็นประจำหรือไม่ หากเป็นเว็บไซต์ระบบธนาคารออนไลน์ จะต้องมี “s” ต่อท้าย https:// ซึ่งหมายถึงการเข้าระบบความปลอดภัย หากไม่มีให้สงสัยว่าเป็นอีเมล์แอบอ้าง นอกจากนี้ หากเป็นการทำธุรกรรมทางการเงิน สถาบันการเงินไม่มีนโยบายในการส่งลิงค์เชื่อมโยงเข้าสู่เว็บไซต์เพื่อทำธุรกรรมทางการเงินผ่านอีเมล์ที่ส่งถึงผู้ใช้บริการ หากมีอีเมล์แอบอ้างแจ้งให้เชื่อมโยงเข้าสู่เว็บไซต์เพื่อทำธุรกรรมทางการเงิน ให้สงสัยว่าเป็นอีเมล์จากมิจฉาชีพ


From: Service PayPal [mailto:paypal@sercuresuite.net]
Sent: 02/21/2008 9:28 AM
To: articles@riverbankconsulting.com
Subject: Service PayPal - Upgrade Your PersonnelAccount information .
PayPal is constantly working to ensure secu
system. We recently reviewed your account
can I restore my account access ?
Click Here, login and com
nexte step ro "Remove Limitations."
Completing all of the infor
ed will automatically restore your account access.
You will be redirct
rivate PayPal server on a random port due security
issues.
PayPal, an eBay company
Copyright 1999-2008 PayPal. All Right reserved.
Information about FDIC pass-through insurance
FAKE EMAIL

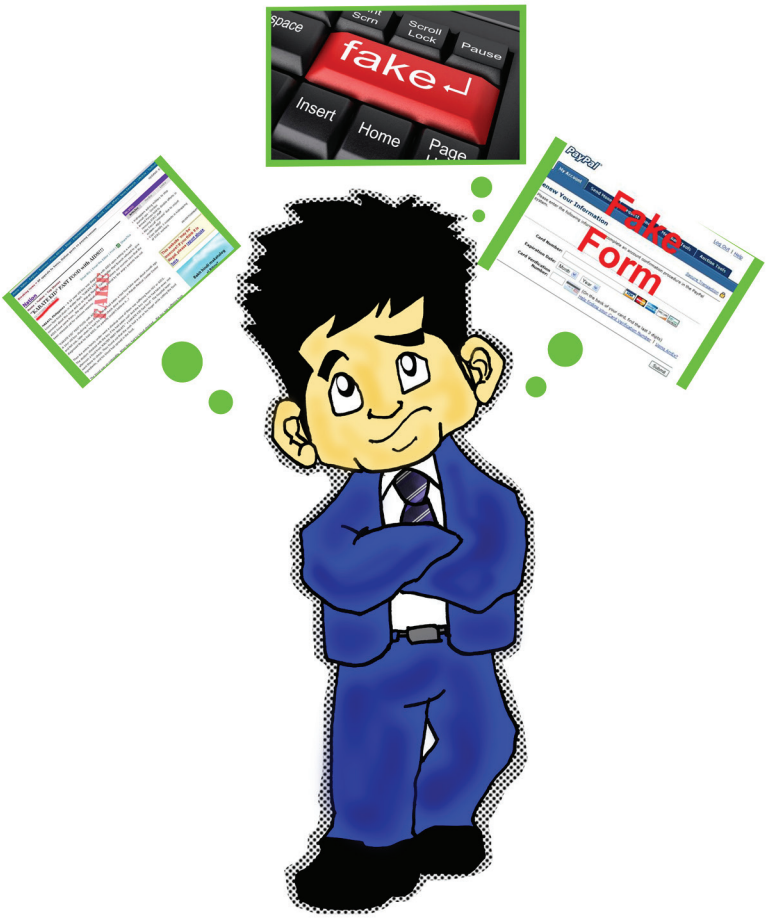
เมื่อได้รับอีเมล์หลอกลวงหรือพบเว็บไซต์ปลอม (Phishing Website) หรือได้กรอกข้อมูลไปในเว็บไซต์ปลอม (Phishing Website) แล้ว ควรติดต่อไปยังหน่วยงาน Call Center ของบริษัท ธนาคาร หรือสถาบันการเงินนั้นๆ โดยเร็วที่สุด เพื่อทำการเปลี่ยนแปลงรหัสผ่าน (Password) หรืออายัดบัญชี เนื่องจากทางบริษัท ธนาคาร หรือสถาบันการเงินไม่มีนโยบายส่งอีเมล์ที่มีลิงค์ให้คลิกเพื่อเข้าสู่ระบบใดๆ ของธนาคาร หรือสอบถามข้อมูลส่วนตัวใดๆ ผ่านทางอีเมล์ หากต้องการเข้าสู่บริการหรือระบบใดๆ จะต้องพิมพ์ที่อยู่ (URL : Uniform Resource Locator) เพื่อเข้าสู่เว็บไซต์ด้วยตัวเอง หรือเข้าจาก Favorite/Bookmark ที่สร้างด้วยตนเองเท่านั้น

ระมัดระวังไม่หลงเชื่อข้อความใดๆ ในอีเมล์หรือโทรศัพท์ที่ได้รับ หากมีการอ้างว่าส่งหรือติดต่อมาจากบริษัท ธนาคาร หรือสถาบันการเงินใดก็ตาม ควรค้นหาหมายเลขโทรศัพท์ของหน่วยงานที่ติดต่อมาหรือติดต่อไปยัง Call Center ของหน่วยงานนั้น (ห้ามติดต่อไปตามหมายเลขโทรศัพท์ที่มีอยู่ในอีเมล์ต้องสงสัยฉบับนั้น) เพื่อทำการตรวจสอบว่ามีการส่งอีเมล์ลักษณะดังกล่าวจริงหรือไม่ หากมีข้อสงสัยสามารถโทรศัพท์สอบถามได้ที่ศูนย์ประสานงานแก้ไขปัญหาการปล่อยสินเชื่อ (ศปส.) ธนาคารแห่งประเทศไทย หมายเลขโทรศัพท์ ๐๒ - ๒๘๓ - ๕๙๐๐ ในวันทำการ ตั้งแต่เวลา ๘.๓๐ – ๑๖.๓๐ น.

ควรลบอีเมล์ที่น่าสงสัยว่ามีไวรัสแนบมา อีเมล์ขยะ อีเมล์ลูกโซ่ หรืออีเมล์ล่อลวงทิ้งทันที อย่าตอบกลับอีเมล์ใดๆ ที่ขอให้เปิดเผยข้อมูลส่วนบุคคล และไม่ควรรันไฟล์ที่แนบมากับอีเมล์ที่ส่งมาจากบุคคลที่ไม่รู้จักหรือไม่ทราบที่มาแน่ชัด ตลอดจนไฟล์ที่ส่งด้วยโปรแกรมแชท (Chat) ต่างๆ



๓. การสังเกตเว็บไซต์ปลอม



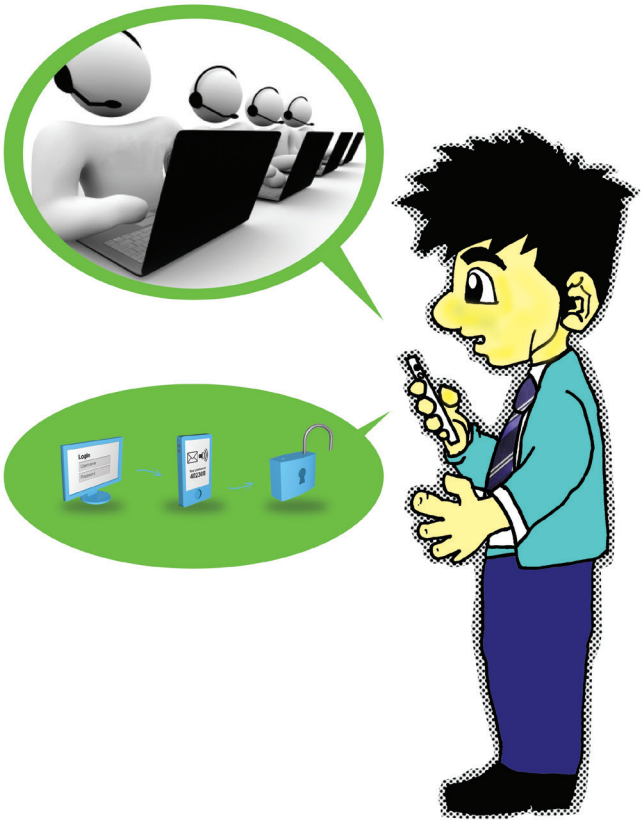
สังเกต “สัญลักษณ์รูปกุญแจ” เพราะระบบธนาคารออนไลน์จะต้องมีการเข้ารหัสความปลอดภัยที่หน้าเว็บไซต์ที่ให้ลงชื่อเข้าใช้ระบบ โดยสัญลักษณ์รูปกุญแจแสดงในส่วนของเว็บบราวเซอร์ (Web Browser) ซึ่งตำแหน่งของสัญลักษณ์อาจแตกต่างกันไปตามประเภทของเว็บบราวเซอร์ (Web Browser)

สังเกต “URL” ของเว็บไซต์ระบบธนาคารออนไลน์ว่ามีการเข้ารหัสความปลอดภัย โดยขึ้นต้นด้วย https:// หรือไม่ หากพบว่าเว็บไซต์ธนาคารออนไลน์ (หน้าลงชื่อเข้าสู่ระบบ) ที่ขึ้นต้นด้วย http:// (ไม่มี s) ให้สงสัยว่าเป็นเว็บไซต์ปลอม

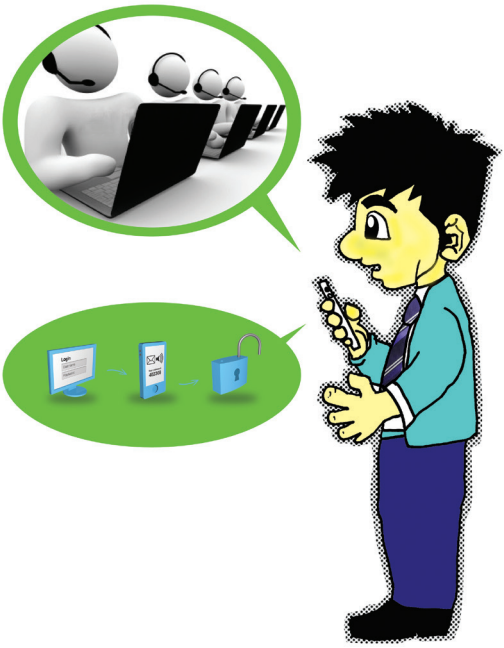
สังเกต “ชื่อผู้ให้บริการ” ว่าถูกจดทะเบียนภายใต้ชื่อสถาบันการเงินใด โดยสามารถสังเกตได้จากตัวอักษรที่อยู่ถัดจากสัญลักษณ์รูปกุญแจ หรือโดยการคลิกที่สัญลักษณ์รูปกุญแจ จะเห็นชื่อสถาบันการเงิน ซึ่งสามารถตรวจสอบดูได้ว่า เป็นชื่อของสถาบันการเงินที่เราใช้บริการหรือไม่

หากพบความผิดปกติของหน้าจอขณะทำรายการผ่านบริการธนาคารออนไลน์ โปรดหยุดทำรายการทันที ไม่ต้องปฏิบัติตามคำแนะนำใดๆ ทั้งสิ้น และกรุณาออกจากเว็บไซต์ที่น่าสงสัยทันที

๔. การใช้รหัสผ่านชั่วคราว OTP (One Time Password) หรือ TOP (Time Out Password)



อ่านข้อความที่ได้รับแจ้งพร้อมรหัสผ่านชั่วคราวจากข้อความที่ส่งผ่านทางโทรศัพท์เคลื่อนที่ (SMS : Short Message Service) ว่ารหัสดังกล่าวใช้ยืนยันการทำธุรกรรมใด หากพบว่าธุรกรรมที่ต้องยืนยันไม่ตรงกับธุรกรรมที่ต้องการทำ ให้ออกจากระบบธนาคารออนไลน์ และติดต่อเจ้าหน้าที่ Call Center ของธนาคารเพื่อปรึกษาการใช้งานที่ปลอดภัยต่อไป



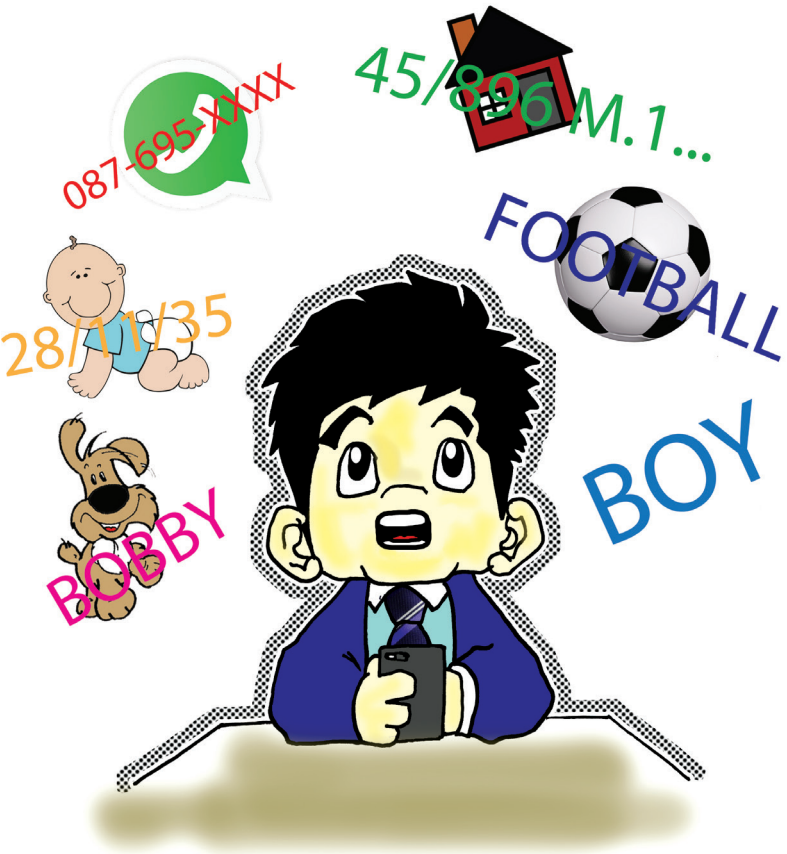
๕. การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

คำแนะนำเกี่ยวกับการตั้งรหัสผ่าน

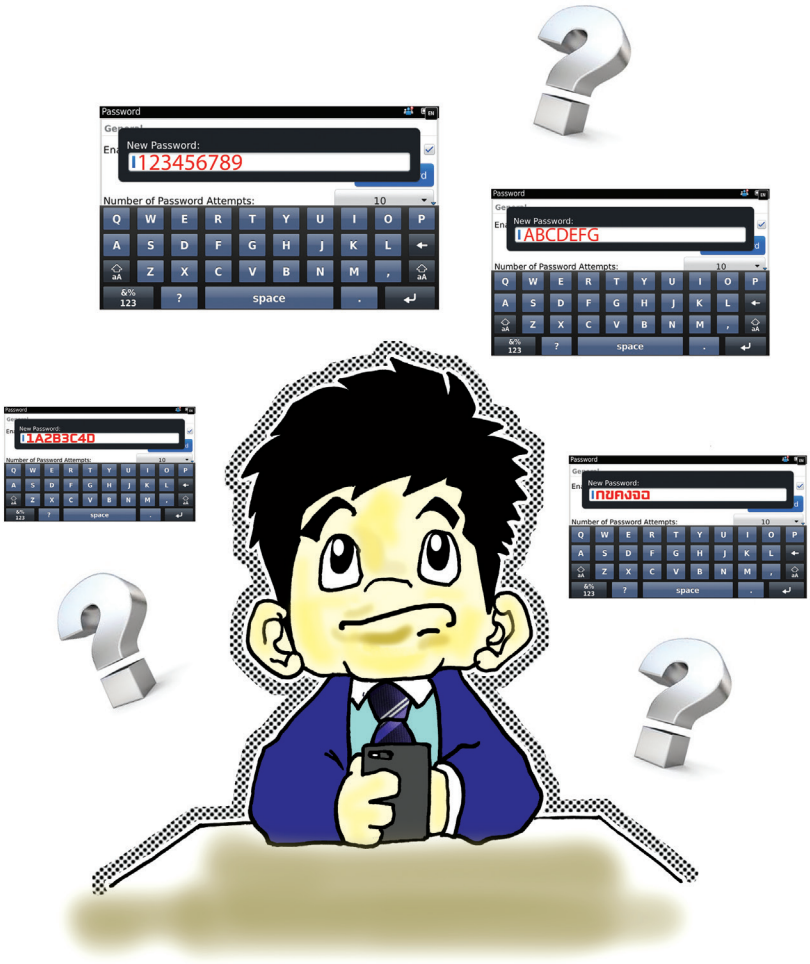
ไม่ใช้คำใดๆ ที่มีอยู่ในพจนานุกรมไม่ว่าจะเป็นพจนานุกรมภาษาใดๆ ก็ตาม รวมทั้งคำศัพท์ทางวิทยาศาสตร์ด้วย

ไม่ใช้คำใดๆ ที่สะกดกลับทาง ซึ่งเป็นคำที่มาจากพจนานุกรม เช่น flower สะกดกลับเป็น rewolf

ไม่ใช้คำใดๆ ที่เกี่ยวข้องกับตัวเรา เช่น ที่อยู่ หมายเลขโทรศัพท์ วันเกิด ชื่อสัตว์เลี้ยง ชื่อเล่น งานอดิเรก หรือกีฬาที่ชอบ

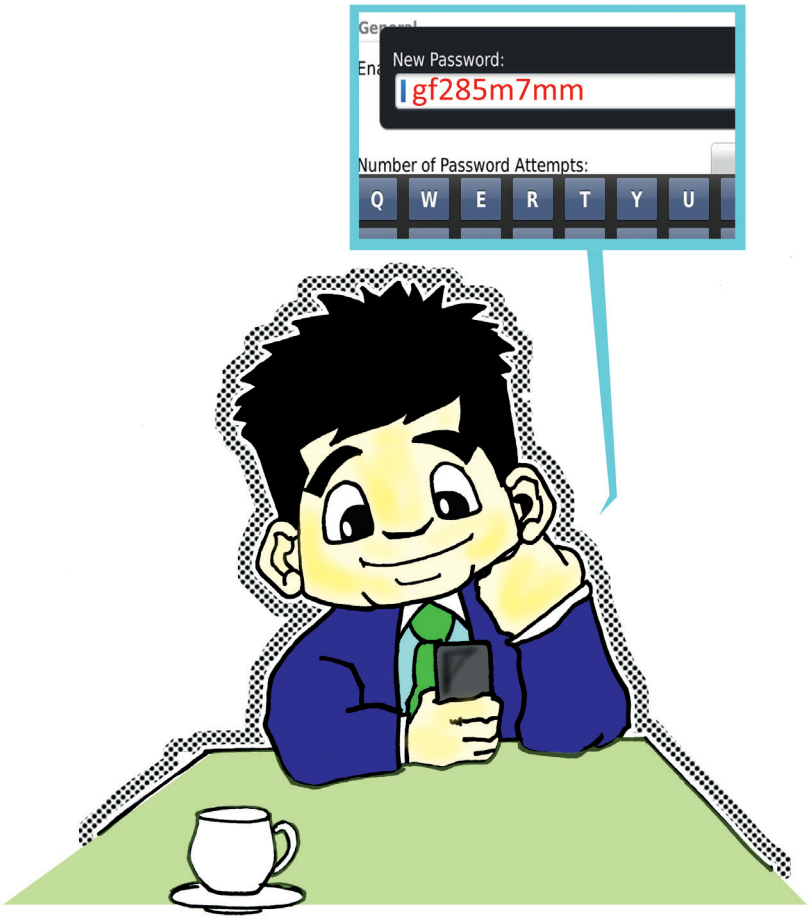


ไม่ใช้ตัวอักษรหรือตัวเลขที่เรียงกัน เช่น “abcdefg” หรือ “1234”

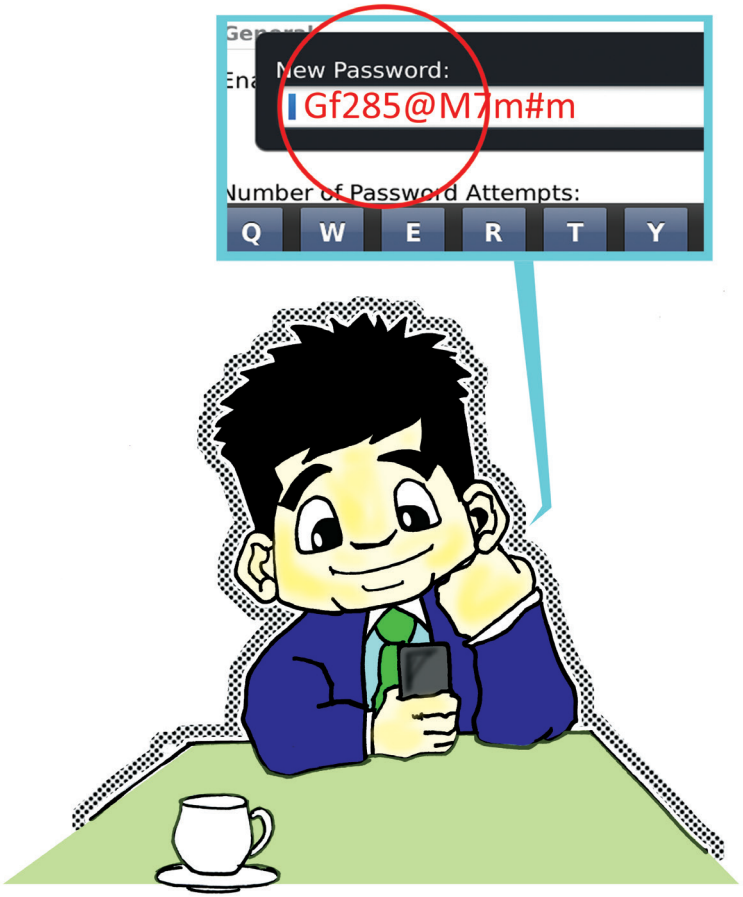


ไม่ใช้ตัวอักษรที่เรียงกันตามแป้นพิมพ์ เช่น “qwerty”

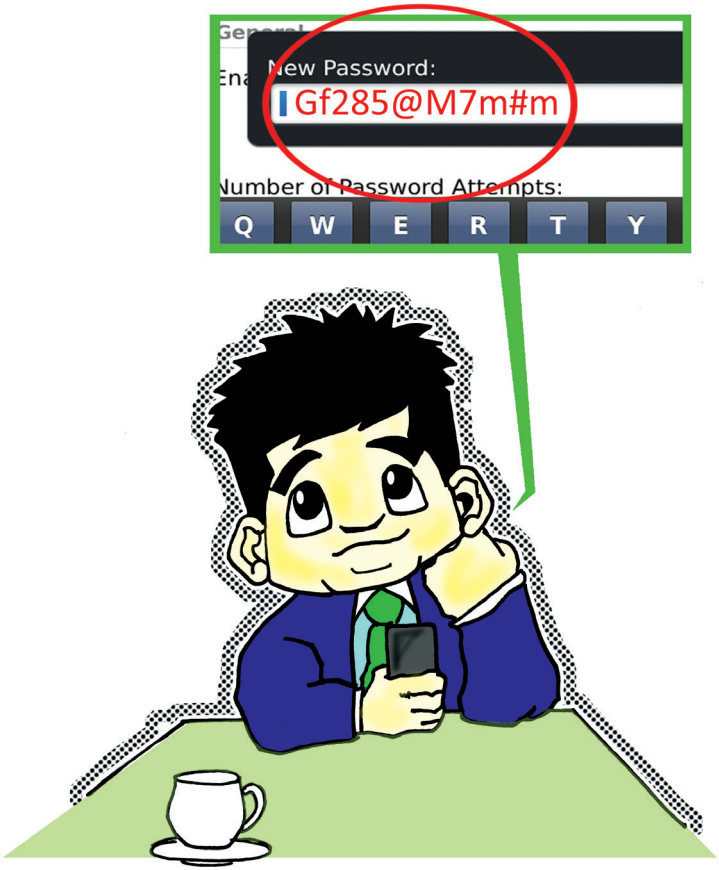
ให้ใช้ตัวอักษร ตัวเลข และตัวอักษรพิเศษร่วมกันแบบสุ่ม



ให้ใช้ตัวอักษรทั้งตัวพิมพ์เล็ก และตัวพิมพ์ใหญ่ในภาษาอังกฤษ และให้ใช้ตัวอักษรพิเศษร่วมด้วย เช่น * @ #

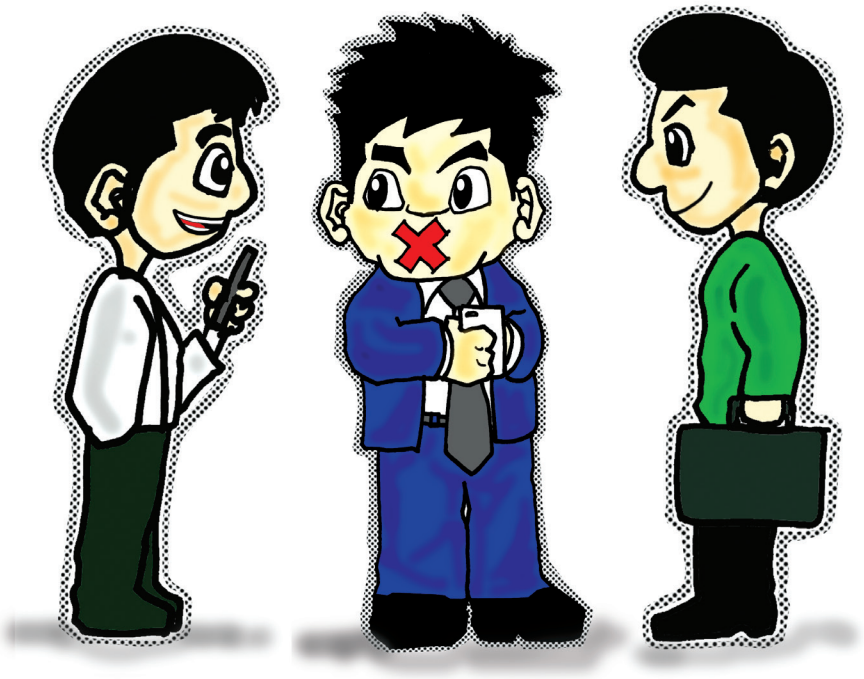


ให้ใช้รหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัว ยิ่งรหัสผ่านมีความยาวเท่าใดก็ยิ่งมีความยากต่อการเดาเท่านั้น



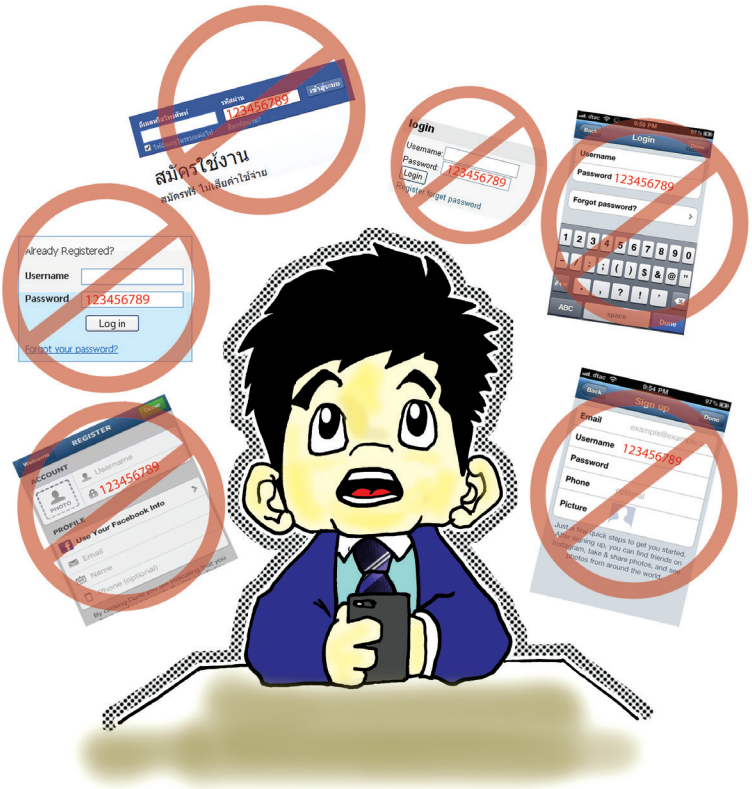
ไม่จดรหัสผ่านเก็บไว้ไม่ว่าจะในที่ใดๆ ก็ตาม และให้ระมัดระวังคนที่นั่งหรือยืนใกล้ๆ ซึ่งอาจแอบมองจากด้านหลังเพื่อขโมยบัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลส่วนตัวอื่นๆ ในขณะที่ผู้ใช้งานกำลังป้อนข้อมูลเหล่านั้นลงในโทรศัพท์เคลื่อนที่

ไม่บอกรหัสผ่านกับผู้อื่นไม่ว่าจะด้วยเหตุผลใดๆ ก็ตาม

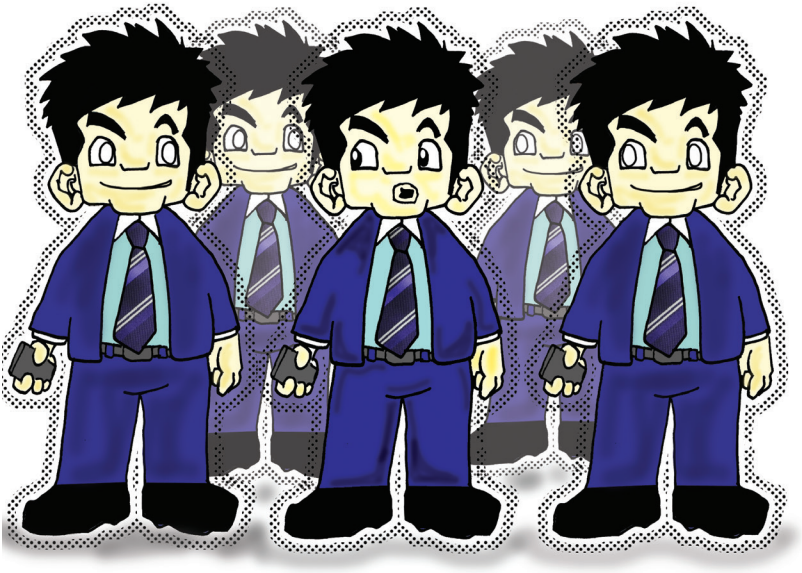


ไม่ใช้ตัวเลือกให้จำรหัสผ่านที่มีอยู่ในเว็บไซต์บางเว็บหรือโปรแกรมที่ใช้งานบางโปรแกรม และให้ปิดความสามารถนี้ในเว็บบราวเซอร์ (Web Browser) ที่ใช้งาน โดยคลิกตัวเลือกการจำรหัสผ่านออก

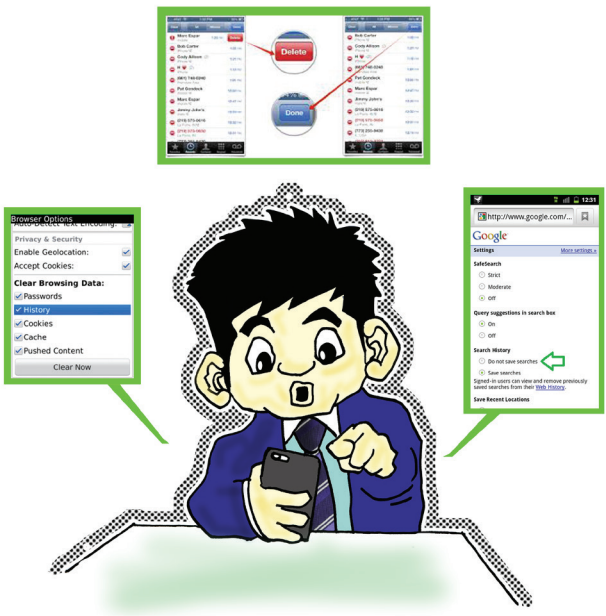
- ไม่ใช้รหัสผ่านเดียวกันเพื่อเข้าใช้งานโปรแกรมต่างๆ



๖. การป้องกันการถูกแอบอ้างใช้งานธนาคารออนไลน์



เมื่อเสร็จการใช้งานในแต่ละครั้ง ควรล้างหน่วยความจำคอมพิวเตอร์ (Cache) และล้างบันทึกประวัติการใช้งาน (History Settings) ในเว็บบราวเซอร์ (Web Browser) เพื่อลบข้อมูลบัญชีทั้งหมด ลดโอกาสที่ผู้อื่นจะสามารถเข้าถึงข้อมูลส่วนตัวได้ และให้ทำการล็อกเอาท์ปิดบราวเซอร์ทั้งหมดที่เปิดใช้งานทุกครั้ง ห้ามละทิ้งโทรศัพท์เคลื่อนที่ไว้หากยังทำธุรกรรมทางการเงินไม่เสร็จ



ไม่ให้ข้อมูลส่วนตัว เช่น หมายเลขบัตรเครดิต เลขที่บัญชีเงินฝาก รหัสผ่านต่างๆ แก่บุคคลอื่น เพราะอาจถูกนำไปใช้แอบอ้างในการทำธุรกรรมทางการเงินได้

ไม่เปิดเผยข้อมูลส่วนบุคคลใดๆ ของตนเอง เช่น รหัสประจำตัว (User ID) รหัสผ่าน (Password) รหัสเอทีเอ็ม (ATM PIN) รหัสบัตรเครดิต หมายเลขบัญชี หมายเลขประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด หรือข้อมูลส่วนบุคคลใดๆ ผ่านทางอีเมล์ หรือในระหว่างทำรายการผ่านบริการของธนาคาร เนื่องจากธนาคารไม่มีนโยบายในการดำเนินการสอบถามข้อมูลส่วนบุคคลใดๆ ของผู้ใช้บริการผ่านช่องทางดังกล่าว


Credit Account
E-Gift Voucher
ยอดที่ชำระรวม: 1,972.60 THB
1-Click - รายการบัตรเครดิตของท่านของท่าน
โอนเงิน
บัญชีผู้โอน
บัญชีผู้รับโอน
จำนวนเงิน (บาท):
1000
วันที่โอนเงิน:
ทันที
ตั้งเวลา
โอนเงินครั้งเดียว
โอนเงินตั้งเวลาแบบครั้งเดียว
12 ธ.ค. 2556
โอนเงินตั้งเวลาแบบประจำ
แจ้งให้ผู้รับโอนทราบผ่านทาง
ยืนยันการโอนเงิน
วัน - เวลาที่ทำรายการ:
11/12/2556 16:55:58
ธนาคารกสิกรไทย
1,000.00
25.00
SMS:
ย้อนกลับ
ตกลง
ยกเลิก

หมั่นตรวจสอบข้อมูลความถูกต้องของการทำรายการธุรกรรมและบัญชีธนาคารทางอินเทอร์เน็ตอย่างสม่ำเสมอ โดยไม่จำเป็นต้องรอให้ครบ ๑ เดือน และตรวจสอบยอดเงินในบัญชีของผู้ใช้บริการอย่างสม่ำเสมอเพื่อป้องกันรายการผิดปกติที่อาจจะเกิดขึ้น รวมทั้งตรวจสอบใบแจ้งรายการใช้บัตรเครดิตทุกครั้งที่ได้รับ และตรวจสอบให้แน่ใจว่าไม่มีรายการธุรกรรมแปลกปลอม หากพบรายการที่น่าสงสัย ให้ติดต่อธนาคารหรือบริษัทผู้ออกบัตรทันที


Checking:
$101.42 (Avail)
$650.42 (Current)
Savings:
$39.52 (Avail)
$44.52 (Current)
SMS Banking
Message No. 4
Your account 'Save 1' was credited with $ 999.98 on Wed 22 Nov 2006
Ref. 2390809CR
Call 800800 for assistance, if required.
Thank you for SMS Banking with ABC Bank.
1:20 pm 22 Nov 2006

หมั่นตรวจสอบข้อความแจ้งเตือนต่างๆ ที่ธนาคารส่งให้ทั้งทางอีเมล์และข้อความที่ส่งผ่านทางโทรศัพท์เคลื่อนที่ (SMS : Short Message Service) อย่างถี่ถ้วน เพื่อให้ทราบถึงความเคลื่อนไหวในบัญชีและการทำธุรกรรมต่างๆ และหากพบความผิดปกติ เช่น หมายเลขบัญชีที่ปรากฏในข้อความไม่ตรงกับหมายเลขบัญชีที่ต้องการลงทะเบียน หรือได้รับข้อความแจ้งเตือนทางอีเมล์โดยที่ไม่ได้เข้าใช้งาน ควรติดต่อธนาคาร สถาบันการเงินนั้นทันที

๗. การติดตามข่าวสารกลโกงและภัยทางการเงิน

ติดตามข่าวสารกลโกงและภัยทางการเงินอย่างสม่ำเสมอ ทั้งจากเว็บไซต์ของธนาคารแห่งประเทศไทย เว็บไซต์ของสถาบันการเงินต่างๆ หรือสื่อสิ่งพิมพ์ต่างๆ เพื่อป้องกันภัยทางการเงินที่อาจเกิดขึ้น

อ้างอิง 

ชัยชนะ มิตรพันธ์ และคนอื่นๆ. **บทความเผยแพร่ Cyber Security Articles 2012 โดย ThaiCERT.** พิมพ์ครั้งที่ ๑. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๖.

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย. **ธนาคารออนไลน์ ใช้งานอย่างไรให้ปลอดภัย.** [ออนไลน์]. เข้าถึงได้จาก : http://www.bot.or.th/Thai/FinancialLiteracy/Documents/ธนาคารออนไลน์ใช้อย่างไรให้ปลอดภัย.pdf. (วันที่ค้นข้อมูล : ๕ กุมภาพันธ์ ๒๕๕๗)

ศูนย์บริหารจัดการความเสี่ยง มหาวิทยาลัยมหิดล. **ระวังโจรออนไลน์ล้วงกระเป๋า.** [ออนไลน์]. เข้าถึงได้จาก : http://www.op.mahidol.ac.th/orau/index.php/articles/60-Risk-Poster/165-Bandit_Online.html. (วันที่ค้นข้อมูล : ๕ กุมภาพันธ์ ๒๕๕๗)

ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี ชั้น ๖
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๕-๙๙
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖-๓๗
เว็บไซต์กระทรวง : http://www.mict.go.th
เว็บไซต์สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ : http://www.etcommission.go.th